AODV Based Black-Hole Attack Mitigation in MANET

Subhashis Banerjee, Mousumi Sardar, and Koushik Majumder

Department of Computer Science and Engineering
West Bengal University of Technology
Kolkata, India
{mail.sb88,mousumi.sardar02}@gmail.com
koushik@ieee.org

Abstract. Packet dropping is a very dangerous attack in case of limited resource networks like Mobile Ad-Hoc Network (MANET). During this attack the malicious node first claims that it has the freshest route to the destination, so the sender selects this as the coordinating node and starts sending data packets to the destination via this node. But afterwards it drops them rather forwarding to the destination. In this paper we give a very clever packet dropping or Black-hole attack detection and prevention technique. Here we use the notion of AODV's sequence number for identifying the Black-hole node in the network. Without using any extra packet or modifying any of the existing packet formats our method can efficiently detect and prevent the Black-hole or packet dropping attack in MANET. All the detection prevention are done by the originator node, so the originator need not relying on the other nodes in the network for this purpose. This method not only detects or prevents the Black-hole attack but is also capable to isolating the Black-hole node from the network.

Keywords: Black-hole attack, AODV, AODV sequence number, Pack dropping attack.

1 Introduction

The Mobile Ad-hoc network (MANET) is dynamically configured network of wireless nodes without any pre-defined infrastructure or centralized authority like wired network. The nodes are very frequent in nature means they can join or leave the network at any time. In MANET, the nodes depend on each other for relaying packets. Due to this uncertain nature of nodes behaviour makes MANET more vulnerable to attacks (active and passive attack [1, 2, and 3]) than wired network. So security becomes an important concern of the network for secure communication. Among the several types of network layer attack, one of the most frequently occurred attack is Black-hole attack. Black-hole attack is an active attack in which malicious node tries to form route towards the destination through itself and later drops packets that are forwarded through it. In this paper we present a mechanism to detect and prevent different types of Black-hole attack. Our mechanism is based on simple Ad-hoc On-demand Distance Vector routing (AODV) protocol.

S.C. Satapathy, S.K. Udgata, and B.N. Biswal (eds.), *FICTA 2013*,
Advances in Intelligent Systems and Computing 247,
DOI: 10.1007/978-3-319-02931-3_39, © Springer International Publishing Switzerland 2014

The remaining part is organized as follows: in section 2 we present an in depth discussion about the Black-hole attack with an example. Next in section 3 we give the literature review. In section 4, our proposed scheme for Black-hole attack detection and prevention is given. Section 5 contains the algorithm. The countermeasure of different types of Black-hole attack with example has been given in section 6 and we finally conclude the paper in section 7.

2 The Black-Hole Attack

During route discovery phase of the AODV [4] routing protocol the source node creates a RREQ packet and broadcasts it in the network. The RREQ packet contains the following information: *1. Destination IP*, *2. Destination Sequence Number*, *3. Originator IP*, *4. Originator Sequence Number*. Sequence Number is a monotonically increasing integer value that is maintained by each originator node. The Sequence Number is used to represent the freshness of the information contained in the packet. During the route discovery phase, in the presence of Black-hole attack, when the malicious node receives RREQ packet, it sends back a RREP packet with a high Sequence Number to indicate that it has the fresher route towards the destination. The source node when receives that RREQ packet it selects that route for having high Sequence Number which is actually contained the malicious node in the path. Then the sender node starts to send packets through that path. On receipt the packets the malicious node start to drop the packets without forwarding it to the destination.

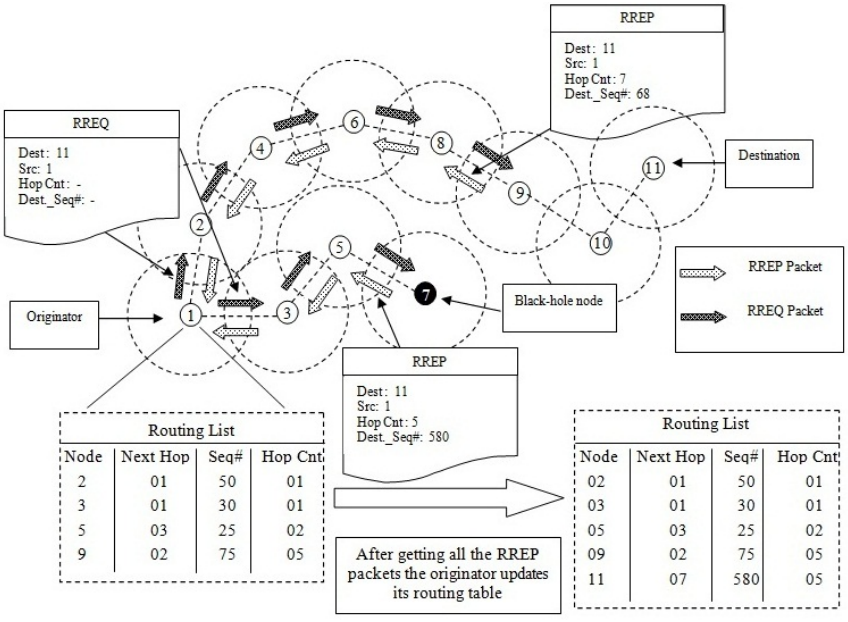

Fig. 1. Example of the Black-hole attack

Consider the MANET with 11 nodes shown in the fig.1. Node 1 is the sender and node 11 is the designated receiver. At first the sender starts the route discovery to discover the best route to the destination. It floods the route request (RREQ) packets in the network as shown in the picture. Now all other nodes including the Black-hole receive the RREQ packet. The node 9 and the Black-hole node (node 7) send the route reply (RREP) packets to the originator. But as displayed in the picture the black hole node does not have a valid path to the destination, and it sends a wrong RREP packet to the sender with a very high sequence number (here sq# is 580) which is much larger than the original one that the node 9 replied (which is 68). So according to the AODV protocol the sender should select the node for further communication that has the best route to the destination, and the freshness of rout is represented through the sequence number in AODV so the originator will select the Black-hole node for the future communication with the destination. And according to its nature the Black-hole node will start dropping the packets received from node 1 rather send it to the destination which is node 11.

3 Literature Survey

S. Marti et al. introduced Watchdog and Pathrater technique [5] to detect and mitigate misbehaviour at time of routing in the network. In Watchdog technique sender node goes into promiscuous mode and listens to its next neighbor node's transmission whether it has been forwarded on or not. If not the node is marked as misbehaving node when the no. of packets not forwarded by the node exceeds a certain threshold. Next based on this knowledge of misbehaving node Pathrater technique is used for choosing the most reliable path. But this technique might not detect a misbehaving node in the presence of a) ambiguous collisions, b) receiver collisions, c) limited transmission power, d) false misbehavior, e) collusion, and f) partial dropping.

S. S. Jain et al proposed a Neighbor monitoring and voting based mechanism [6] for detecting and removing the malicious nodes that launch Black-hole or Gray-hole attacks. In this mechanism the whole traffic is divided into a set of small data blocks. Before sending data packets sender node sends prelude message to inform destination about the incoming packet. After that it broadcasts monitor message to inform all the nodes in the path to start monitoring its next node. After that sender node starts to send data packets. On receiving the prelude message destination starts timer and counts the no. of data packets it received and sends back this information to source node by postlude message. In this way after getting postlude message within timeout period the sender node compares the no. of sent packets with no. of received packets. If both are same it sends the other data blocks to the destination. Otherwise it starts a malicious node detection and removal process by the help of voting mechanism. If the voteCount for a node exceeds predefined thresholdCount the node is marked as malicious node by the sender node. This method successfully detect and prevent the cooperative Black-hole and Gray-hole attacks in O(n) time but a hypothetical assumption that a neighbor node of any node is more trusted than malicious nodes make it quite impractical.

R. Shree et al. proposed Secure-ZRP [7] to detect and prevent Black-hole attack. A special packet 'bluff probe' is used to identify the Black-hole node. This packet contains a non-existent destination ID and broadcasts by the sender before forwarding the actual route request packet. The Black-hole node will sends back a reply when it receives that packet through intermediate node while the good nodes will forward the packet to its next neighbor as their routing table doesn't contain the fake destination ID. This is only detection technique that is applicable on both proactive and reactive protocol. But it cannot detect Gray-hole attack and every node has to maintain valid route table that impose too much overhead.

M. Al-Shurman et al. proposed Redundant Route Method and Unique Sequence Number Scheme [8] in which the safe route is selected on the basis of RREP packet observation that whether the two or more routes have same shared hop or not. If any route doesn't have any shared hops sender node waits for another RREP packet until a routes with shared node is identified or routing timer expires. From this shared nodes information sender prevents the Black-hole attack and selects the safe route.

A detailed literature survey on Wormhole attack and their existing countermeasures with a comparison can be found in our previous work [9].

After the survey work we find that many of the existing detection or prevention techniques modify the packet format by adding some extra fields in it or introduce some new packets. Many of them assume that the sender can control the intermediate nodes, and intermediate nodes will do many extra works like observing the behaviour of its neighbours in favor of the sender. But in the practical scenario this cannot be possible.

Here we propose a Black-hole detection and prevention technique that does not modify the packet format of existing routing protocol, and also does not introduce new packet. The sender can do all the detection and prevention process by itself. Our method only uses an extra route discovery phase for finding the Black-hole node. But this extra route discovery is an optimized route discover phase because during it the originator does not flood the complete network with the RREQ packets, it only multicast the RREQ packet along some routes from which it previously gets RREP packets.

4 Proposed Method for Black-Hole Attack Detection and Prevention

Our proposed Black-hole attack detection and prevention method consists of the following two phases: 1) Black-hole node identification phase. 2) Black-hole node removal phase.

4.1 Black-Hole Node Identification Phase

After the originator receives all the RREP packets it finds the packet which contains the largest sequence number from its cache. Now the originator creates new RREQ

packets for the same destination node with a higher destination sequence number than the sequence number that the RREP packet contains which it receives previously from an intermediate node. Now the originator multicasts the packets through the route from which it gets the RREP packets.

According to the AODV protocol when a new RREQ sent by node S for a destination is assigned a higher destination sequence number. The intermediate nodes which know a route, but with a smaller sequence number, cannot send the RREP packet to the sender. Now all the intermediate nodes that receive the RREQ packet compare its destination sequence number for the same destination with the destination sequence number that the RREQ packet contains. As the sender used a false destination sequence number that is higher than all the destination sequence number that all the nodes have there should not be any RREP coming from any intermediate nodes. If any one of the intermediate node is malicious then according to its nature it will sends the RREP packets that have a higher destination sequence number than the RREQ packet contains for attracting the sender. When the sender receives that RREP packet, it confirms that this is a Black-hole node. The originator now selects the node that previously replied with the next height sequence number among the nodes that did not change its sequence number during the false RREQ propagation, for future communication to the receiver.

If there is no RREP during the false RREQ packet transmission the originator selects the node that has replied with the height sequence number during the first route discovery phase. When a Black-hole node is detected then the sender starts the Black-hole node removal process as follows:

4.2 Blackhole Node Removal Phase

Once the originator detects that there is a Black-hole node in the network, it adds it IP address in its malicious node table and avoid the node in future communication. And we assume that the nodes in the network periodically exchange the malicious node table, so other nodes in the network also aware of the Black-hole node.

5 Proposed Algorithm

Now we give the algorithm for detecting and preventing the Black-hole attack. Without any packet modification or imposing to much over head the sender can efficiently detect and prevent the Black-hole attack, as well as the Black-hole node is isolated from the network by our malicious node list exchange procedure. Our algorithm consists of the following two procedures:

1. Black-hole node identification during the route discovery phase of the AODV routing protocol.
2. Black-hole node removal from the network.

Procedure 1 : *Black-hole node identification during the route discovery phase of the AODV routing protocol*

Step 1: Originator initiates the route discovery by flooding the RREQ packets.
Step 2: Originator receives the RREP packets from other nodes in the network which have a valid path to the receiver.
Step 3: Originator stores all the RREP packets in its cache.
Step 4: Then the originator selects the RREP packet that has the maximum sequence number and extracts its sequence number in a variable called max.
Step 5: Now the originator creates new RREQ packets for the same destination node with a higher destination sequence number than the value of max.
Step 6: The originator also sets the hop count value of the RREQ packet to maximum of the distance of the replying nodes.
Step 7: Then it multicasts the new RREQ packet towards all paths from which it receives route replies during the first route discovery phase.
Step 8: Originator waits for a time span for RREP packets.
Step 9: If (*there is RREP packets with higher destination sequence number than that it sends*)
9.1. The nodes that replied height sequence number is a Black-hole node and wants to carry out a packet dropping attack by giving the wrong information.
9.2. Next the originator invokes the Black-hole node removal procedure (present in the next part of the algorithm).
9.3. The originator selects the node that previously replied with the next height sequence number among the nodes that did not replied during the false RREP propagation, for future communication to the receiver.
9.4. Sender starts to sends the data packets via the selected reliable route after the Black-hole removal process.
Step 10: Else
// There is no black hole node in the network
10.1. Sender selects the forward path that has been established during the first RREP propagation form the sender to the intermediate node that has replied with the freshest route to the destination.
10.2. Sender starts to send the data packets via the selected route to the destination.
Step 11: End.

Procedure2 *: Black-hole node removal from the network*

Step 1: Add the IP address of the Black-hole node in the originators malicious node list.
Step 2: Every time after the malicious node list has been updated, the node shares its malicious node list with its neighbours.
Step 3: Nodes in the network avoid the nodes that are in the malicious node list for forwarding the data.
Step 4: End.

6 Black-Hole Attack Detection and Removal

Now we will explain how does our proposed method detect and remove the Black-hole node from the network with an example. Consider the MANET displayed in the fig. 1. After the route discovery phase, the originator receives all the RREP packets, and stores them in cache. Now it selects the packet with the highest sequence number and store the sequence number in a variable called max. In Our example the node 7 (Black-hole node) replied with the maximum Dest._Seq#, which is 580.

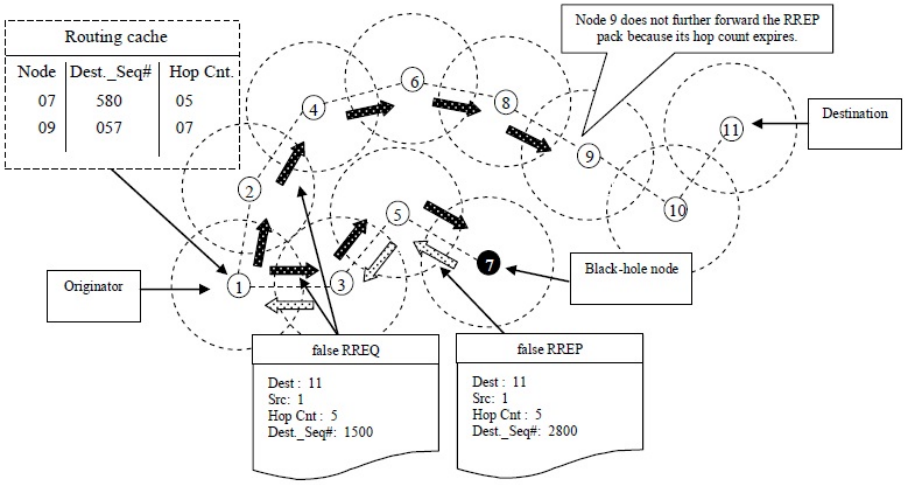

Fig. 2. Originator floods the false RREQ packs for finding the Black-hole node

Now according to our algorithm the sender starts the Black-hole node detection procedure. It first creates new RREQ packet with the Dest._Seq# set to a value greater than 580, which is in our example 1500 and sets the hop count to 5. Source selects the route through node 7 with hop count 5 because the node 9 has the maximum distance from the source. Now the originator sends the packet to node 11 via two different paths one is via 1→3→5→7, and another is via 1→2→4→6→8→9 (fig.2).

Consider the fig. 2 where the Black-hole node sends a false RREP packet corresponding to the false RREQ claiming that it has a better route towards the destination. In our example it sends a RREP packet that has a greater Dest._Seq# value (i.e., 2080) than the false one sent by the source. Now after receiving the RREP packet from the suspected node the originator gets confirm that this is a Black-hole node. So now the originator adds its id in the malicious node list and carries out the Black-hole node removal procedure. Next the originator selects node 9 for the future communication with the receiver, because it does not replied in the false route request.

Also note that our method is capable to detect the Black-hole nodes if there is more than one in the network. We think this is the main advantage of our method because as per our knowledge there is no detection or prevention scheme that can detect more than one Black-hole nodes if they present in the network.

7 Conclusion and Future Work

In this paper we present an initial work in detecting and mitigating the Black-hole attack in a theoretical and algorithmic point of view. Here we have proposed an efficient packet dropping attack prevention technique, which is the super-ordinate or generalized form of all types of Black-hole attacks. The main strength of the proposed method is that, it does not either modify the packet format of AODV or introduce any kind of new Black-hole detection packets like its predecessors. This method can efficiently detect all types of Black-hole attacks such as single and cooperative Black-hole attacks and also isolates the black-hole node from the network. The extra overhead that our method imposes on the network is very minimal with only an additional route discovery phase. And also we optimize the second route discovery by multicasting the RREQ packets without broadcasting that. As a result, the data packets reach the destination successfully, which is a sensitive issue in this type of limited resource network.

References

1. Nguyen, H.L., Nguyen, U.T.: A study of different types of attacks on multicast in mobile ad hoc networks. Ad Hoc Networks 6(1), 32–46 (2008)
2. Karmore, P., Bodkhe, S.: A Survey on Intrusion in Ad Hoc Networks and its Detection Measures. International Journal on Computer Science and Engineering, IJCSE (2011)
3. Rai, A.K., Tewari, R.R., Upadhyay, S.K.: Different Types of Attacks on Integrated MANET-Internet Communication. International Journal of Computer Science and Security, IJCSS 4(3) (2010)
4. Perkins, C.E., Belding-Royer, E.M., Das, S.R.: Ad hoc on-demand distance vector (AODV) routing. RFC 3561, The Internet Engineering Task Force, Network Working Group (2003), http://www.ietf.org/rfc/rfc3561.txt
5. Marti, S., Giuli, T.J., Lai, K., Baker, M.: Mitigating routing misbehavior in mobile ad hoc networks. In: Proceedings of the 6th Annual International Conference on MOBICOM, Boston, Massachusetts, United States, pp. 255–265 (2000)
6. Jain, S., Jain, M., Kandwal, H.: Advanced algorithm for detection and prevention of cooperative black and Grayhole attacks in mobile ad hoc networks. J. Computer Applications 1(7), 37–42 (2010)
7. Shree, R., Dwivedi, S.K., Pandey, R.P.: Design Enhancements in ZRP for Detecting Multiple Blackhole Nodes in Mobile Ad Hoc Networks. International Journal of Computer Applications 18(5), 6–10 (2011)
8. Al-Shurman, M., Yoo, S.M., Park, S.: Blackhole Attack in Mobile Ad Hoc Networks. In: Proceedings of the 42nd Annual ACM Southeast Regional Conference, ACM-SE'42, Huntsville, Alabama (April 2004)
9. Banerjee, S., Majumder, K.: A Comparative Study on Wormhole Attack Prevention Schemes in Mobile Ad-Hoc Network. In: Thampi, S.M., Zomaya, A.Y., Strufe, T., Alcaraz Calero, J.M., Thomas, T. (eds.) SNDS 2012. CCIS, vol. 335, pp. 372–384. Springer, Heidelberg (2012)